Yevseyeva I, Fernandes VB, van Moorsel A, Janicke H, Emmerich M.

Two-stage security controls selection.

In: International Conference on ENTERprise Information Systems/International Conference on Project MANagement/International Conference on Health and Social Care Information Systems and Technologies, CENTERIS/ProjMAN / HCist 2016.

5-7 October 2016, Porto, Portugal: Elsevier BV.

Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 100 (2016) 971 – 978

Procedia Computer Science

Conference on ENTERprise Information Systems / International Conference on Project MANagement / Conference on Health and Social Care Information Systems and Technologies, CENTERIS / ProjMAN / HCist 2016, October 5-7, 2016

Two-stage security controls selection

Iryna Yevseyeva[a*], Vitor Basto Fernandes[b], Aad van Moorsel[c], Helge Janicke[a], Michael Emmerich[d]

[a] *Cyber Technology Institute, Faculty of Technology, De Montfort University, Gateway House, The Gateway, LE1 9BH Leicester, UK*
[b] *School of Technology and Management, Computer Science and Communications Research Centre, Polytechnic Institute of Leiria, Leiria 2411-901, Portugal*
[c] *Centre for Cybercrime and Computer Security, School of Computing Science, Newcastle University, Newcastle upon Tyne NE1 7RU, UK*
[d] *LIACS, Leiden University, Niels Bohrweg 1, 2333-CA Leiden, The Netherlands*

Abstract

To protect a system from potential cyber security breaches and attacks, one needs to select efficient security controls, taking into account technical and institutional goals and constraints, such as available budget, enterprise activity, internal and external environment. Here we model the security controls selection problem as a two-stage decision making: First, managers and information security officers define the size of security budget. Second, the budget is distributed between various types of security controls. By viewing loss prevention with security controls measured as gains relative to a baseline (losses without applying security controls), we formulate the decision making process as a classical portfolio selection problem. The model assumes security budget allocation as a two objective problem, balancing risk and return, given a budget constraint. The Sharpe ratio is used to identify an optimal point on the Pareto front to spend the budget. At the management level the budget size is chosen by computing the trade-offs between Sharpe ratios and budget sizes. It is shown that the proposed two-stage decision making model can be solved by quadratic programming techniques, which is shown for a test case scenario with realistic data.

Peer-review under responsibility of the organizing committee of CENTERIS 2016

Keywords: multicriteria optimisation; security; subset selection; security budget; portfolio optimization; Sharpe ratio

* Corresponding author. Tel.: +441162577540; fax: +441162577540.
E-mail address: iryna.yevseyeva@dmu.ac.uk

Peer-review under responsibility of the organizing committee of CENTERIS 2016
doi:10.1016/j.procs.2016.09.261

1. Introduction

Industry needs to protect its assets, products and business processes from potential cyber security breaches in order to maintain its business functions. This boils down to the selection of security *controls* or *countermeasures*, aimed at either blocking an attack or mitigating damage from a successful attack. Potential threats come from hackers aiming at attacking random users and companies, e.g. via spam and social engineering attacks, e.g. phishing, viruses and trojans, spyware and malware, botnets, etc. or targeting particular companies or individuals, e.g. via distributed denial of service (DDoS), spear phishing, ransom ware and other brute force or low rate attacks. Especially dangerous are complex persistent attacks that aim at disrupting the normal functioning of a particular company, exploiting several vulnerabilities at once.

The race between attackers, who are constantly searching for vulnerabilities and antivirus software producers, who are constantly patching vulnerabilities, continues. Despite continuous increase of investments in security by large companies, regular media reports about emergent attacks, security breaches, and the increasing scale of economic losses, demonstrate that the problem of security is far from being solved.

The 2015 information security breaches survey [1] conducted by PwC for UK government reported that 90% of large and 74% of small organizations suffered security breaches in 2014, an increase from the previous year from 81% and 60%, respectively. The average worst single security breach cost went up from £600k - £1.15m in 2014 to £1.46m - £3.14m in 2015 for a large organization and from £65k - £115k in 2014 to £75k - £311k in 2015 for a small business. 59% of respondents expect an increase of security incidents in the upcoming years, suggesting an increase in security budgets to prevent and to mitigate security breaches. Similar trends are reported for businesses in the US, see e.g. Ponemon Institute report [2].

In this context companies face at least two problems: Firstly, to decide on the budget for secure functioning of the company; secondly, to divide the budget among security controls to buy and to update. Another interesting issue, which is beyond the scope of this paper, is how to act in the case of a breach: which countermeasures to apply when an attack happens and how to perform incident response most efficiently.

The problem of choosing a budget to be spent is a management decision, usually made by the board of directors/owners of company together and is informed by Chief Information Security Officer (CISO). The decision making involves estimating risks related to potential attacks and security breaches, and considering how well other competitor companies are protected. In business it is believed that it is enough to be protected slightly better than competitors in order to reduce the chances of being attacked, since attackers search for easiest targets [3].

The problem of allocating budget between different security controls is solved by the CISO, who usually follows security policies of the company and existing standards for risk assessment, e.g. [4, 5]. Decisions about which controls to buy would typically be done with a limited budget and it is not possible to buy all available controls.

Existing risk assessment models are based on qualitative or quantitative analysis or some combination of both. For instance, international standards ISO/IEC 27001/2 [6] and NIST [7] provide general recommendations for qualitative risk assessment. In [8] both approaches are used, qualitative (for identifying groups of attackers or assigning levels of attack severity) and quantitative (for measuring efficiency of countermeasures against various threats and their cost). Both of the indicated problems have been addressed in the literature, but not solved together. Recent approaches to risk assessment and planning address minimizing security risk and budget for controls simultaneously [12], applying financial modelling for risk assessment [11], planning under uncertainty for high impact events [15], formulating budget allocation as a multiple knapsack problem [16,17]. In our previous work [18], several alternative formulations for selecting the optimal subset of security controls were suggested.

In this paper, we extend work started in [18] and address two stages of security controls selection problem: the security budgeting and selection of security controls given such budget. In Section 2, state-of-the art approaches are considered for both indicated problems and in Section 3 we propose our approach to solving these problems. The presented approach is illustrated with an example in Section 4. We draw conclusions and indicate future directions for this work in Section 5.

2. Budget and security controls selection

One of the main challenges in the security industry is the difficulty of demonstrating and quantifying the benefit of security investments to convince managers to invest in security. The difficulties in defining cyber-security create confusion and a lack of public understanding of cyber security threats [19]. Hence, potential resistance of managers to invest into cyber security may be related to such luck of understanding. To help managers to make informed decision about the security budget, several educational sessions about security threats may be organized. In this section an approach for helping managers on security budget selection and its allocation between security controls is proposed based on portfolio selection problem well known in financial management.

2.1. Budget selection

In budget selection, one considers securing a company as a rewarding activity, e.g. by viewing loss prevention with security controls as gains relative to a baseline (without them). Such activity requires some resources and leads to potentially prevention of serious loss, e.g. in case if highly improbable but very damaging new type of attack is prevented saving the company from high losses or even bankruptcy. We believe that this viewpoint will help managers when allocating security budget and find security investment as potentially profitable. Hence, in these settings there will always be some security budget that the company wants to spend for security. However, there will still be the question, which is the best value for it taking into account size of the company, its activity, how much the company invested into security before and how much it wants to spend for updating old and buying new security controls. Currently most CISOs/managers look at other companies and implement similar to competitors' security measures [3]. It is also believed that it is enough to be protected slightly better than competitors to be out of the attackers focus.

There might be conflicts of opinions between different managers and/or CISO, which make agreeing about the budget of the company difficult. Solutions for this problem can be found with the help of group decision-making approaches, see e.g. [14]. After the budget for protecting company from potential attacks is chosen by top managers, CISO has to make decisions about how to spend the allocated budget wisely.

2.2. Traditional security risk

A large number of potential threats exist that might happen with some probability to any company, governmental organization or individuals. Security experts can subjectively evaluate the probability or likelihood of each threat based on their experience and knowledge of recent threats and attacks by analyzing existing vulnerabilities of valuable company's assets. In addition to the probability/likelihood of a threat, a typical risk assessment procedure will take into account the impact of exploitation.

The most common way CISOs take to perform risk assessment of the company is by assessing expected loss value. The initial loss value L, when no security controls are applied, can be computed, e.g. similarly to [12], by analyzing existing vulnerabilities of the company's assets $V_i \in \{0,1\}$, estimating probabilities/likelihood $p_{ij} \in [0,1]$ of exploiting vulnerabilities V_i via potential threats $T_j \in \{0,1\}$ and impact of such exploitations $I_i \in \{10,50,100\}$, where $i=\{1,\ldots,n\}$ and $j=\{1,\ldots,m\}$ indicate vulnerabilities and threats, respectively:

$$L = \sum_{j=1}^{m} \sum_{i=1}^{n} p_{ij} \cdot V_i \cdot I_i \,. \tag{1}$$

Investment in the security budget should be done in such a way to minimize potential losses. To spend the available budget B from all available controls $l=\{1,\ldots,k\}$ some should be selected to be bought $x_l \in \{0,1\}$ (where 1 stands for selecting l-th control to be bought and 0 for not selecting) and leading to integer formulation of the portfolio selection problem (when compared to standard continuous). Let x denote the choice of subset of controls, e.g. $x = (0,1,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)^T$ means that x_2 and x_5 controls are selected (bought). For this the CISO has to evaluate how well each control x_l protects each vulnerability V_i. See Table 3 for such values $t_{li} \in \{-1,-0.5,0,0.5,1\}$ as suggested in [12]. Note that negative values of t_{li} show that new risks are introduced by using control, $t_{li}=0$ if control x_l is not covering vulnerability V_i, and complete cover with $t_{li}=1$.

$$P(x) = \sum_{k=1}^{l} \sum_{j=1}^{m} \sum_{j=1}^{n} p_{ij} \cdot V_i \cdot I_i \cdot t_{li} \cdot x_l \,. \tag{2}$$

The total cost C is usually composed from direct and indirect costs of security controls (for buying and maintaining them, respectively), where c_l is the cost of the security control x_l.

$$C(x) = \sum_{l=1}^{k} x_l \cdot c_l \,. \tag{3}$$

Then, such subset of security controls has to be selected that minimizes the total loss/risk after applying controls $R(x) = L - P(x)$ taking into account constrained budget B:

$$\min_{x_l} R(x) \;\; s.t. C(x) \le B \,. \tag{4}$$

However, it is not always possible to evaluate security in terms of reducing risk of potential losses and view these losses independently from each other. Here we suggest an alternative view that considers prevention of losses as gains relative to the baseline of not investing in security. This change of view allows us to consider the selection of security controls as well as the budget allocation problem as an investment portfolio optimization problem with positive return on investment and variance of return on investments.

2.3. Security risk vs. rewarding security

We propose to approach investment into security as a profitable activity that would encourage managers to invest into. An example of profitable investment into security can be considered when an attack has been prevented by one of company's employees; such prevention can also be seen as a gain for the company since big loss has been prevented. Then investing time, effort and other resources needed for detection and prevention of an attack is seen as necessary spending/investment for avoiding potentially big losses.

In the above-discussed settings CISO is interested in allocating the available budget into best controls, i.e. the controls with maximal total efficiency of protecting the company against as many as possible known and desirably unknown potential threats. This will maximize the expected return or gain from the investment. Note that controls with high protection efficiency against potentially as many threats as possible are preferred to those with low protection efficiency against smaller number of threats. Hence, coverage of as many as possible threats is encouraged intrinsically within individual controls' efficiency (by covering many threats). Then, expected return (which is not necessary monetary) of a set of security controls can be computed as the difference between gains obtained from implementing controls and their costs:

$$E(x) = G(x) - C(x). \tag{5}$$

There are different ways to define gain. For instance, it can be taken as $P(x)$ defined by (2). The larger the value of the expected gain the better the company is protected from potential threats, and a subset of security controls x_l which maximizes gain should be selected.

2.4. Diverse controls selection

At the same time threats coverage can also be taken into account extrinsically by comparing how different sets of controls cover sets of threats. Traditionally in financial world investing into similar financial assets is risky [9], since similar assets or industries might loose their value for the same reasons, e.g. oil and gas becomes cheaper due to new types of energy production advances so investing in only those two industries is risky. Similarly when selecting several species of biological population for future preservation, e.g. several plants species for their potential future (yet unknown) pharmaceutical benefit, it is important to select as diverse species as possible [10].

In security (to account for diversity) it is assumed that controls of the same type/kind would provide protection against similar type of threats. Then, in order to protect a company from various threats, various or diverse types of controls should be selected and selecting similar ones is considered to be risky. Following the classical financial model of Markowitz [9], the risk $\sigma(x)$ can be expressed in terms of the covariance matrix Q as follows

$$\sigma(x) = \sqrt{\sum_{l=1}^{k}\sum_{s=1}^{k}\sum_{i=1}^{m} x_l \cdot q_{lsi} \cdot x_s} \,. \quad (6)$$

As above x denotes the choice of subset of controls. Each element q_{lsi} of matrix Q represents how similar are two controls x_l and x on vulnerability V_i. It should be possible for CISO to evaluate covariance (similarity) values q_{lsi} based on pairwise comparison of controls. Note that negative covariance (e.g. $q_{lsi} = -1$) shows dissimilarity between controls and is preferable, contrary to positive covariance (e.g. $q_{lsi} = 1$), which should be avoided, and risk term $\sigma(x)$ is to be minimized.

Then, such a subset of security controls has to be selected that maximizes the expected return from applying selected controls $E(x)$ and minimizes risk of selecting similar controls $\sigma(x)$ simultaneously, taking into account limited budget.

$$\max E(x) \quad and \quad \min \sigma(x) \;\; s.\,t. \quad C(x) \le B \,. \quad (7)$$

Note that there may be several of such optimal subsets, selecting one among which is not trivial.

2.5. Risk-to-Return trade-offs for different budgets

Optimizing (7) leads to finding not a single but multiple so-called Pareto optimal subsets of controls each of which is better on at least one of the objectives (return or risk) and not worse on the rest of objectives. To select one solution among many, various approaches can be taken, for instance one of them is to find an optimal ratio between risk and return subject to budget constraint. For instance, return-to-risk Sharpe ratio well known in financial literature [13] can be used here:

$$\max Sh(x) = \frac{E(x)}{\sigma(x)}, \quad s.\,t. \quad C(x) \le B \,. \quad (8)$$

The maximization of the Sharp ratio typically leads to a so-called knee point solution on the Pareto front, which is a point in which the losses as compared to the best attainable value for both objectives (here expected return and standard deviation) are small. Quadratic programming techniques can be used to determine points on the Pareto front. Among these points the point with maximal Sharpe ratio can be found either by enumeration or by geometrical construction. For the latter, indifference lines can be constructed and among them the line tangential to the Pareto frontier, the so-called Capital Allocation Line (CAL), determines the point with optimal Sharp ratio on the Pareto front.

3. Experimental results

Next, we exemplify this strategy by means of a realistic example. The scenario and data are taken from [12]. 24 possible security controls can be applied, all of which with a specific cost and protecting more or less effectively for a certain set of security vulnerabilities. Moreover, in some cases they have an averse effect on the protection, e.g. while protecting for one type of vulnerability opening up the possibility of certain other types of vulnerabilities.

As stated above, the selection of controls is modeled by means of a binary decision vector and the aim is to find the optimal selection with respect to the Sharpe ratio. Recall the expected return $E(x)$ is the expected gain $G(x)$ minus cost $C(x)$. In this example a simplified version of gain is considered. It is assumed that if control x_l is selected, the gain will be the sum of all vulnerability impacts I_i times the effectiveness t_{il} (matching) of control x_l on vulnerability V_i. The precise data can be obtained from Tables 1-3.

Table 1 Impact of Vulnerabilities

Vulnerability	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}
Impact on CIA	PPP	PPP	CCC	PPP	PPP	NNP	PPP	CCC	PPP	CCC
Impact I_i/£100	50	50	100	50	50	10	50	100	50	100

Table 2 Costs of controls (countermeasures)

Control (x_l)	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
Cost/£100	25	31.8	12	5	18.5	2.1	4	19	34	1.5	5.5	46

Control (x_l)	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}
Cost/£100	7.6	25	10	23	60	11.5	25	40	7	26	20	43

Table 3. Effectiveness of security controls' protection of vulnerabilities

		Vulnerabilities (V_i)									
	t_{li}	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}
Controls (x_l)	x_1	1	0	-0.5	0	0.5	0	-0.5	-0.5	0	-0.5
	x_2	0	0	-0.5	0	0.5	-0.5	-0.5	0	0.5	0.5
	x_3	1	0.5	-0.5	0.5	1	1	1	1	0.5	0.5
	x_4	-0.5	0	-1	0	1	1	1	1	0.5	0.5
	x_5	0.5	0	-1	0	0.5	0	0.5	0.5	-0.5	-0.5
	x_6	0.5	0	-0.5	0	0	0	0	0.5	0	0
	x_7	0	0.5	-0.5	0	0.5	0	0	1	0	0
	x_8	0	0	-0.5	0	0.5	0	0	0	0	0
	x_9	0	0	0	0	1	0	0.5	0.5	-0.5	-0.5
	x_{10}	0	0	-1	0	1	0	0.5	0.5	-0.5	0.5
	x_{11}	0.5	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5	-0.5
	x_{12}	0.5	0.5	-0.5	0	0	0	0.5	0.5	1	0.5
	x_{13}	0	1	0	0.5	0	0.5	0	0.5	0	0
	x_{14}	0	0	0.5	0	0	0	1	0.5	0	0
	x_{15}	0	0	0.5	0	0.5	0	0	0	0	0.5
	x_{16}	1	0.5	1	0.5	0.5	0.5	1	1	1	1
	x_{17}	0.5	0.5	-0.5	0.5	1	0.5	0.5	0.5	1	1
	x_{18}	1	1	1	0.5	0.5	0.5	0.5	0.5	0.5	0.5
	x_{19}	0.5	0.5	-0.5	0	-0.5	0	0	0.5	0	0
	x_{20}	-0.5	0	-0.5	0	0	0	0	0	0	0
	x_{21}	0	1	0	0.5	0	0	0	0	0.5	0
	x_{22}	1	0	-1	0	0	0	0	0	0	0
	x_{23}	0	-0.5	0	0	0.5	0	0.5	0	0	0
	x_{24}	-0.5	0	-1	0	0	0	0	0	0	0

Now $E(x) = G(x) - C(x)$ with $G(x) = \sum_{l=1}^{24}\left[\sum_{i=1}^{10} t_{li} \cdot I_i\right] \cdot x_l$ and $C(x) = \sum_{l=1}^{24} C_l \cdot x_l$. The return of a single control is given by $r_l = \left[\sum_{i=1}^{10} t_{li} \cdot I_i\right] - C_l$ and total expected return is $E(x) = (r_1, \ldots, r_{24}) \cdot x$. The covariance of the return can be computed as: $Q_{ls} = Cov((t_{l1} \cdot I_1 - C_l, \ldots, t_{l10} \cdot I_{10} - C_l), (t_{s1} \cdot I_1 - C_s, \ldots, t_{s10} \cdot I_{10} - C_s))$ which is equivalent to $Q_{ls} = \frac{1}{n^2} \sum_{l=1}^{24} \sum_{s=1}^{24} \frac{1}{2}((t_{li} \cdot I_i - C_l) - (t_{si} \cdot I_i - C_s))((t_{lz} \cdot I_z - C_l) - (t_{sz} \cdot I_z - C_s))$.

Given a maximal budget B that can be spent on controls we can solve the Sharpe index optimization problem.

$$Sh(x) = \frac{G(x) - C(x) - r_0}{\sqrt{\sigma^2(x)}} \to \max, \ \text{s. t.} \ \sum_{l=1}^{24} C_l \cdot x_l \le B. \tag{9}$$

where r_0 is risk free return, which we assume here to be equal to 0, i.e. r_0=0.

For solving the formulation (9) with integer variables $x_l \in \{0,1\}$, here MATLAB quadratic solver is used [20]. The results are shown in Figure 1 (left and right). Here we illustrate return to variance Pareto front and Maximal Sharpe ratio for different variance, respectively.

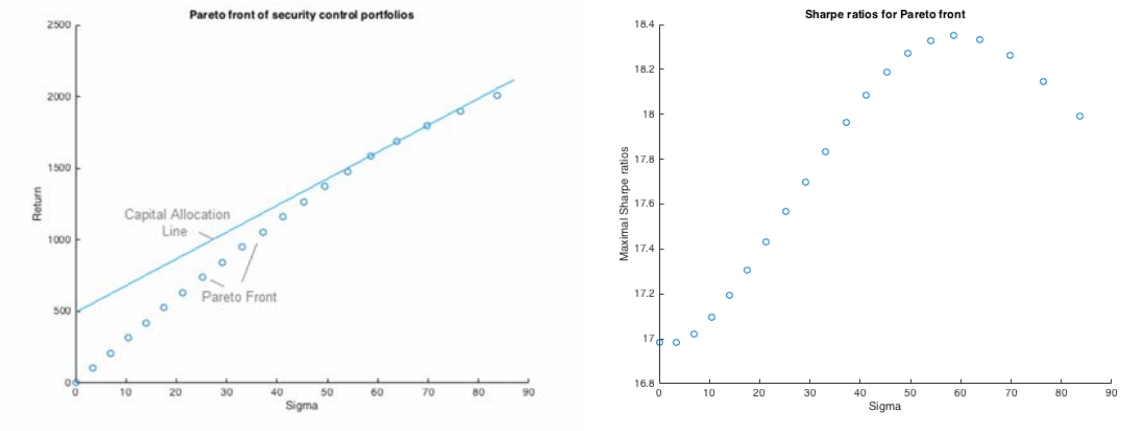

Figure 1 Pareto front of security control portfolios and maximal Sharpe ratios

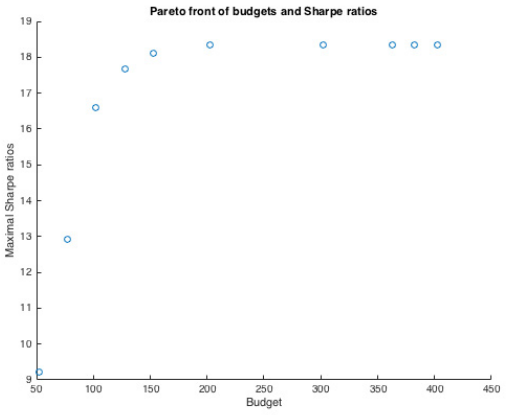

Figure 2 Pareto front of budgets vs. maximal Sharpe ratios

Figure 1 (left) shows also the Capital Allocation Line (CAL), which is tangential to the Pareto front in the point of the maximal Sharpe ratio. This is confirmed by Figure 1 (right), where at a value of about $\sigma(X)$=60 the curve reaches the maximal value of Sharpe ratio.

An advantage of a single-number performance index for a budget allocation, as it is provided with the Sharpe ratio, is that it can be used for supporting top-level decision-making using techniques from multi-criteria decision-making. For this we propose to compute the Pareto front of budgets and optimal Sharpe ratios that can be achieved for these budgets and present this to the top-level decision maker. Here MATLAB solver was used to compute Pareto front [20]; alternative exact solvers could be used [19]. The problem can be solved efficiently, as budget is a constant and different values of it can be chosen in an interval from 0 to the maximal possible budget. Thereafter, for each budget the maximal Sharpe ratio is computed, which gives rise to an approximation of the Pareto front. The results for the example are shown in Figure 2.

Clearly budgets above £25.000 do not improve anymore the performance measured by Sharpe ratio. A sharp drop in performance is observed for values below £12.500. The advice would be that investments below this value would deteriorate security performance significantly. The knee point region on the Pareto front between £12.500 to circa £15.000 represents good choices of security budgets.

4. Conclusion

In this research we discuss the problem of security controls selection from a managerial point of view. It is advocated to view the implementation of security controls as a profitable investment. By viewing the scenario of not using any security controls as the baseline scenario, it is possible to assign positive gains to security investments, which puts us into the position to apply classical and well-established tools from financial investment theory to the problem of selecting security controls. These tools balance risk and return in an optimal way, e.g. by maximizing the Sharpe ratio. From our example it becomes clear that the strategy can be implemented based on realistic data. Moreover, it is efficient to compute such portfolios and it allows for a well-informed multi-criteria assessment of alternatives. Besides offering a method for CISOs to allocate a given budget, the Pareto front of the Sharpe ratio (to be maximized) to the security budget (to be minimized) can be used to make decisions on the right budget assigned to security in a company.

References

1. 2015 Information security breaches survey. Published in March 2015 by PWC in association with InfoSecurity Europe https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf.
2. 2015 Cost of Cyber Crime Study: United States Published in October 2015 by Ponemon Institute http://www.ponemon.org/library/2015-cost-of-cyber-crime-united-states.
3. Huber M, Buttermann A, Trigo LD, Möller M, Dornbusch P, Zundt M, editors: IT-security in global corporate networks.. Trend report 2002. Center for Digital Technology & Market.
4. 10 Steps to cyber security: executive companion. BIS/12/1120. Published on 5 September 2012. https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility
5. Mobile Devices. Guide for Implementers. Published in February 2013. MWR InfoSecurity. https://www.cpni.gov.uk/Documents/Publications/Non-CPNI_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf
6. ISO/IEC 27002, Information Technology – Security Techniques – Code of practice for information security management, 2005. http://www.iso.org/iso/catalogue_detail?csnumber=50297
7. NIST National vulnerability database, automating vulnerability management, security measurement and compliance checking http://nvd.nist.gov/home.cfm.
8. Thomas L, Norman Risk Analysis and Security Countermeasure Selection 2nd ed. Boca Raton: CRC Press Taylor and Francis Group; 2016.
9. Markowitz H, Portfolio selection, *Journal of Finance* 1952;7(1):77-91.
10. Solow A, Polasky S, Measuring biological diversity, *Environmental and Ecological Statistics* 1994;1:95-107.
11. Sawik T., Selection of optimal countermeasure portfolio in IT security planning, *Decision Support Systems* 2013;55:156-164.
12. Viduto V, Maple C, Huang W, López-Peréz D, A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem, *Decision Support Systems* 2012;53(3) 599-610
13. Sharpe WF. The Sharpe ratio, *The journal of portfolio management* 1994; 21(1): 49-58.
14. Belton V, Stewart T, Multiple Criteria Decision Analysis: An Integrated Approach, Kluwer Academic Publishers, Dordrecht; 2002.
15. Rakes TR, Deane J.K., Rees L.P., IT security planning under uncertainty for high-impact events, *Omega* 2012;40(1):79-88.
16. Smeraldi F. Malacaria P, How to spend it: optimal investment for cyber security, In Proceedings of the 1st International Workshop on Agents and CyberSecurity (ACySE '14). ACM, New York, NY, USA, May 5th 2014.
17. Fielder A, Panaousis E, Malacaria P, Hankin P, Smeraldi F, Decision support approaches for cyber security investment, *Decision Support Systems*, 2016; 86, 13-23.
18. Yevseyeva I, Basto-Fernandes V, Emmerich MTM, van Moorsel A, Selecting Optimal Subset of Security Controls, Procedia Computer Science, 2015; 64, 1035-1042.
19. Masin M, Bukchin Y, Diversity maximization approach for multiobjective optimization. Operations Research, 2008; 56(2):411-424.
20. MATLAB, 2015, version R2015b, The MathWorks Inc. Natick, Massachusetts.